10/661,650

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

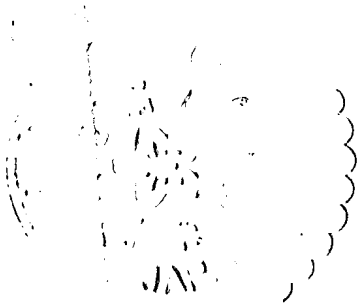
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１０月１１日

出願番号
Application Number: 特願２００２－２９９７２１

[ST. 10/C]: [ＪＰ２００２－２９９７２１]

出願人
Applicant(s): 株式会社リコー



２００３年　８月２７日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０６９７６３

【書類名】　特許願
【整理番号】　0206874
【提出日】　平成14年10月11日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 12/00　537
【発明の名称】　電子ファイル管理装置
【請求項の数】　7
【発明者】
【住所又は居所】　東京都大田区中馬込１丁目３番６号
株式会社リコー内
【氏名】　斉藤　敦久
【特許出願人】
【識別番号】　000006747
【氏名又は名称】　株式会社リコー
【代表者】　桜井　正光
【代理人】
【識別番号】　100084250
【弁理士】
【氏名又は名称】　丸山　隆夫
【電話番号】　03-3590-8902
【手数料の表示】
【予納台帳番号】　007250
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　0207936
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電子ファイル管理装置

【特許請求の範囲】

【請求項１】　データを受け取って管理する管理手段と、

前記受け取ったデータがオリジナル電子ファイルだけからなるのか、電子ファイルへのアクセス権限を管理するための情報を含むアクセス権限情報とオリジナル電子ファイルとからなるのかを判定する判定手段と、

前記アクセス権限情報を付加されたオリジナル電子ファイルであった場合に、該オリジナル電子ファイルからアクセス制限をかけたアクセス制限電子ファイルを生成するアクセス制限手段と、

前記オリジナル電子ファイル、または／及び該オリジナル電子ファイルとアクセス制限電子ファイルとアクセス制限情報とを格納する格納手段と、を備え、

前記管理手段は、前記オリジナル電子ファイルと、当該オリジナル電子ファイルから生成されたアクセス制限電子ファイルとを、当該オリジナル電子ファイルに対するアクセス権限情報に基づいて管理することを特徴とする電子ファイル管理装置。

【請求項２】　データを受け取って管理する管理手段と、

前記受け取ったデータがオリジナル電子ファイルだけからなるのか、電子ファイルへのアクセス権限を管理するための情報を含むアクセス権限情報とオリジナル電子ファイルとからなるのかを判定する判定手段と、

前記アクセス権限情報を付加されたオリジナル電子ファイルであった場合に、該オリジナル電子ファイルからアクセス制限をかけたアクセス制限電子ファイルを生成するアクセス制限手段と、

前記オリジナル電子ファイル、または／及び該オリジナル電子ファイルとアクセス制限電子ファイルとアクセス制限情報とを格納する格納手段と、を備え、

前記管理手段は、前記オリジナル電子ファイルと、当該オリジナル電子ファイルから前記アクセス制限手段により生成されたアクセス制限電子ファイルとを当該オリジナル電子ファイルに対するアクセス権限情報に関連付けて前記格納手段に格納し、アクセス要求を受けると、前記アクセス権限情報に基づいて前記オリ

ジナル電子ファイル又は前記アクセス制限電子ファイルを前記格納手段から出力する／出力しないことを特徴とする電子ファイル管理装置。

【請求項３】　データを受け取って管理する管理手段と、

前記受け取ったデータがオリジナル電子ファイルだけからなるのか、電子ファイルへのアクセス権限を管理するための情報を含むアクセス権限情報とオリジナル電子ファイルとからなるのかを判定する判定手段と、

前記アクセス権限情報を付加されたオリジナル電子ファイルであった場合に、該オリジナル電子ファイルからアクセス制限をかけたアクセス制限電子ファイルを生成するアクセス制限手段と、

前記オリジナル電子ファイル、または／及び該オリジナル電子ファイルとアクセス制限電子ファイルとアクセス制限情報とを格納する格納手段と、を備え、

前記管理手段は、前記オリジナル電子ファイルから前記アクセス制限手段によりアクセス制限電子ファイルが生成されると、該オリジナル電子ファイルを破棄して生成されたアクセス制限電子ファイルを前記格納手段に格納し、アクセス要求を受けると、アクセス制限電子ファイルを前記格納手段から出力することを特徴とする電子ファイル管理装置。

【請求項４】　前記管理手段は、アクセス制限電子ファイルを当該アクセス制限電子ファイルに対するアクセス権限情報に関連づけて前記格納手段に格納し、アクセス要求を受けると、前記アクセス権限情報に基づいて前記アクセス制限電子ファイルを前記格納手段から出力する／出力しないことを特徴とする請求項３記載の電子ファイル管理装置。

【請求項５】　データを受け取って管理する管理手段と、

前記受け取ったデータがオリジナル電子ファイルだけからなるのか、電子ファイルへのアクセス権限を管理するための情報を含むアクセス権限情報とオリジナル電子ファイルとからなるのかを判定する判定手段と、

前記アクセス権限情報を付加されたオリジナル電子ファイルであった場合に、該オリジナル電子ファイルからアクセス制限をかけたアクセス制限電子ファイルを生成するアクセス制限手段と、

前記オリジナル電子ファイル、または／及び該オリジナル電子ファイルとアク

セス制限電子ファイルとアクセス制限情報とを格納する格納手段と、を備え、

前記管理手段は、前記オリジナル電子ファイルを当該オリジナル電子ファイルに対するアクセス権限情報に関連付けて前記格納手段に格納し、アクセス要求を受けると、該アクセス権限情報に基づいて、前記アクセス制限手段にアクセス制限電子ファイルを生成させて出力する／出力しないことを特徴とする電子ファイル管理装置。

【請求項６】　データを受け取って管理する管理手段と、

前記受け取ったデータがオリジナル電子ファイルだけからなるのか、電子ファイルへのアクセス権限を管理するための情報を含むアクセス権限情報とオリジナル電子ファイルとからなるのかを判定する判定手段と、

前記オリジナル電子ファイル、または該オリジナル電子ファイルとアクセス制限電子ファイルとアクセス制限情報とを格納する格納手段と、を備え、

前記管理手段は、オリジナル電子ファイルと、当該オリジナル電子ファイルに対するアクセス権限情報と、該アクセス権限情報でアクセス権限を認められているユーザのみが復号可能であるよう該オリジナル電子ファイルを暗号化したアクセス制限電子ファイルとを受け取って前記格納手段に格納し、アクセス要求を受けると、前記アクセス権限情報に基づいて前記オリジナル電子ファイル又は前記アクセス制限電子ファイルを前記格納手段から出力する／出力しないことを特徴とする電子ファイル管理装置。

【請求項７】　前記アクセス制限電子ファイルは、暗号化された後ＩＤを付けられ、該ＩＤに基づいてアクセス権限情報との対応を確認されることを特徴とする請求項１から６の何れか１項に記載の電子ファイル管理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、例えば技術文書などの電子ファイルを管理し、アクセス権限に応じて活用できるようにする電子ファイル管理装置、方法、プログラム、及び該プログラムを記録した記録媒体に関する。

【０００２】

【従来の技術】

従来より、電子ファイルを管理する電子ファイル管理装置では、格納する電子ファイルに対して予めパスワードを登録させ、ユーザからのアクセス要求を受けると、そのユーザが登録されたパスワードを入力した場合にのみ、そのパスワードに対応する電子ファイルを表示装置や外部記憶装置に出力する。

【０００３】

また、本出願人により先に出願されている特開２００１－１４２８７４号公報（特許文献１）の「文書管理システム」は、電子化された文書を作成して登録し、承認されるとその文書を変換して印刷可能なＰＤＦと印刷不可能なＰＤＦとを作成し、利用権限に応じて閲覧できるファイルを制限するものである。

【０００４】

【特許文献１】

特開２００１－１４２８７４号公報

【０００５】

【発明が解決しようとする課題】

しかしながら、従来の電子ファイル管理装置では、アクセス権限を認められたユーザが電子ファイルを取得した後、アクセス権限を認められていないユーザに取得した電子ファイルを渡すと、アクセス権限を認められていないユーザであってもその電子ファイルにアクセスできてしまうという問題があった。

【０００６】

また、上述した特許文献１の文書管理システムは、電子化された文書を利用権限を認められていないユーザに対しても閲覧のみを許可しつつ印刷を不可能とする好適なものであるが、利用権限を認められているユーザが印刷可能なＰＤＦを読み出した後、他の利用者にその印刷可能はＰＤＦを渡してしまうと、本来印刷可能なＰＤＦへのアクセス権限のない利用者でもＰＤＦを印刷することができてしまっていた。

【０００７】

本発明はこのような状況に鑑みてなされたものであり、オリジナルのドキュメントと、ユーザの権限に応じたアクセス制限を施した保護ドキュメントとをアク

セス権限に応じて適切に管理することができる電子ファイル管理装置、方法、プログラム、及び該プログラムを記録した記録媒体を提供することである。

【０００８】

【課題を解決するための手段】

係る目的を達成するために請求項１記載の発明は、データを受け取って管理する管理手段と、受け取ったデータがオリジナル電子ファイルだけからなるのか、電子ファイルへのアクセス権限を管理するための情報を含むアクセス権限情報とオリジナル電子ファイルとからなるのかを判定する判定手段と、アクセス権限情報を付加されたオリジナル電子ファイルであった場合に、該オリジナル電子ファイルからアクセス制限をかけたアクセス制限電子ファイルを生成するアクセス制限手段と、オリジナル電子ファイル、または／及び該オリジナル電子ファイルとアクセス制限電子ファイルとアクセス制限情報とを格納する格納手段と、を備え、管理手段は、前記オリジナル電子ファイルと、当該オリジナル電子ファイルから生成されたアクセス制限電子ファイルとを、当該オリジナル電子ファイルに対するアクセス権限情報に基づいて管理することを特徴とする。

【０００９】

請求項２記載の発明は、請求項１記載の発明において、データを受け取って管理する管理手段と、受け取ったデータがオリジナル電子ファイルだけからなるのか、電子ファイルへのアクセス権限を管理するための情報を含むアクセス権限情報とオリジナル電子ファイルとからなるのかを判定する判定手段と、アクセス権限情報を付加されたオリジナル電子ファイルであった場合に、該オリジナル電子ファイルからアクセス制限をかけたアクセス制限電子ファイルを生成するアクセス制限手段と、オリジナル電子ファイル、または／及び該オリジナル電子ファイルとアクセス制限電子ファイルとアクセス制限情報とを格納する格納手段と、を備え、管理手段は、前記オリジナル電子ファイルと、当該オリジナル電子ファイルから前記アクセス制限手段により生成されたアクセス制限電子ファイルとを当該オリジナル電子ファイルに対するアクセス権限情報に関連付けて前記格納手段に格納し、アクセス要求を受けると、前記アクセス権限情報に基づいて前記オリジナル電子ファイル又は前記アクセス制限電子ファイルを前記格納手段から出力

する／出力しないことを特徴とする。

【００１０】

請求項３記載の発明は、データを受け取って管理する管理手段と、受け取ったデータがオリジナル電子ファイルだけからなるのか、電子ファイルへのアクセス権限を管理するための情報を含むアクセス権限情報とオリジナル電子ファイルとからなるのかを判定する判定手段と、アクセス権限情報を付加されたオリジナル電子ファイルであった場合に、該オリジナル電子ファイルからアクセス制限をかけたアクセス制限電子ファイルを生成するアクセス制限手段と、オリジナル電子ファイル、または／及び該オリジナル電子ファイルとアクセス制限電子ファイルとアクセス制限情報とを格納する格納手段と、を備え、管理手段は、前記オリジナル電子ファイルから前記アクセス制限手段によりアクセス制限電子ファイルが生成されると、該オリジナル電子ファイルを破棄して生成されたアクセス制限電子ファイルを前記格納手段に格納し、アクセス要求を受けると、アクセス制限電子ファイルを前記格納手段から出力することを特徴とする。

【００１１】

請求項４記載の発明は、請求項３記載の発明において、管理手段は、アクセス制限電子ファイルを当該アクセス制限電子ファイルに対するアクセス権限情報に関連づけて前記格納手段に格納し、アクセス要求を受けると、前記アクセス権限情報に基づいて前記アクセス制限電子ファイルを前記格納手段から出力する／出力しないことを特徴とする。

【００１２】

請求項５記載の発明は、データを受け取って管理する管理手段と、受け取ったデータがオリジナル電子ファイルだけからなるのか、電子ファイルへのアクセス権限を管理するための情報を含むアクセス権限情報とオリジナル電子ファイルとからなるのかを判定する判定手段と、アクセス権限情報を付加されたオリジナル電子ファイルであった場合に、該オリジナル電子ファイルからアクセス制限をかけたアクセス制限電子ファイルを生成するアクセス制限手段と、オリジナル電子ファイル、または／及び該オリジナル電子ファイルとアクセス制限電子ファイルとアクセス制限情報とを格納する格納手段と、を備え、管理手段は、前記オリジ

ナル電子ファイルを当該オリジナル電子ファイルに対するアクセス権限情報に関連付けて前記格納手段に格納し、アクセス要求を受けると、該アクセス権限情報に基づいて、前記アクセス制限手段にアクセス制限電子ファイルを生成させて出力する／出力しないことを特徴とする。

【００１３】

請求項６記載の発明は、データを受け取って管理する管理手段と、受け取ったデータがオリジナル電子ファイルだけからなるのか、電子ファイルへのアクセス権限を管理するための情報を含むアクセス権限情報とオリジナル電子ファイルとからなるのかを判定する判定手段と、オリジナル電子ファイル、または該オリジナル電子ファイルとアクセス制限電子ファイルとアクセス制限情報とを格納する格納手段と、を備え、管理手段は、オリジナル電子ファイルと、当該オリジナル電子ファイルに対するアクセス権限情報と、該アクセス権限情報でアクセス権限を認められているユーザのみが復号可能であるよう該オリジナル電子ファイルを暗号化したアクセス制限電子ファイルとを受け取って前記格納手段に格納し、アクセス要求を受けると、前記アクセス権限情報に基づいて前記オリジナル電子ファイル又は前記アクセス制限電子ファイルを前記格納手段から出力する／出力しないことを特徴とする。

【００１４】

請求項７記載の発明は、請求項１から６の何れか一項に記載の発明において、アクセス制限電子ファイルは、暗号化された後ＩＤを付けられ、該ＩＤに基づいてアクセス権限情報との対応を確認されることを特徴とする。

【００１５】

【発明の実施の形態】

次に、本発明に係る電子ファイル管理装置、方法、プログラム、及び該プログラムを記録した記録媒体を、図面を用いて詳細に説明する。

まず、本発明の実施形態としての電子ファイル管理装置における、各実施形態に共通する概要について説明する。

【００１６】

本発明の実施形態としての電子ファイル管理装置は、装置本体と、ユーザが入

力を行う入力手段と、ユーザに対して各種の情報を表示する表示手段とを備えて構成される。

上記の入力手段は、例えばキーボードやマウスなどであり、表示手段は、例えばディスプレイなどである。

装置本体は、オリジナルのドキュメント（Document；オリジナル電子ファイル）と保護ドキュメント（Protected Document；アクセス制限電子ファイル）との管理を行い、入力手段から操作を行うユーザに認められたアクセス権限に応じて上記の表示手段に出力する。

装置本体からの出力先は上記の表示手段に限定されず、例えばプリンタを装置本体に接続することで、そのプリンタから印字（出力）することもできる。また、ユーザからのアクセス要求がＦＤ（フロッピー（登録商標）ディスク）などのリムーバブルディスクといった情報記録媒体への保存である場合には、その情報記録媒体に保存することとしてよい。

【００１７】

次に、本発明の第１の実施形態としての電子ファイル管理装置２について説明する。

この第１の実施形態は、ドキュメント管理プログラム（Document Management Program）２１を用いてドキュメント１１（オリジナルのドキュメント；オリジナル電子ファイル）、またはドキュメント１１とＡＣＬ（Access Control List；アクセス権限情報）１２とを保存した際に、保護ドキュメント１３を作成して、基本的にその保護ドキュメント１３にのみアクセスさせるモデルである。

【００１８】

第１の実施形態における装置本体２ａは、ドキュメント１１、またはドキュメント１１とＡＣＬ１２とを受け取って管理するドキュメント管理プログラム（管理手段）２１と、ドキュメント１１とＡＣＬ１２とからアクセス制限をかけた保護ドキュメント１３を生成するドキュメント保護プログラム（Document Protection Program ；アクセス制限手段）２２と、電子ファイル（各種ドキュメントやＡＣＬなど）を格納するドキュメント管理ＤＢ（Document Management DB；格納手段）２３と、をＨＤＤなどの記憶部（不図示）に備えてなる。

上記のＡＣＬ１２は、ドキュメント１１へのアクセス権限を管理するための情報を含むものである。

【００１９】

この第１の実施形態の装置本体２ａは、物理的には、各種のプログラムやデータなどを記憶する上記した記憶部と、ＣＰＵなどの主制御部とを備えて構成され、この主制御部が記憶部に格納されたプログラムにより処理を行うことで、この装置本体２ａは上述した管理手段と、アクセス制限手段と、格納手段として機能する。

すなわち、電子ファイル管理装置２は、上記の記憶部に記憶されたドキュメント管理プログラム２１により主制御部が処理を行うことで上記した管理手段として機能し、上記の記憶部に記憶されたドキュメント保護プログラム２２により主制御部が処理を行うことで、上記したアクセス制限手段として機能する。

【００２０】

ＡＣＬ１２の構成例を図２に示す。この図２に示す例では、ＡＣＬ１２は、ユーザ名（User name ）、アクセスタイプ（Access type ）、許可情報（Permission）及び処理要件（Requirement ）をパラメータとして構成される。

すなわち、何らかのアクセス権限を認められたユーザのユーザ名（User name ）に、そのユーザに認められたアクセス権限が、ユーザからの操作命令（Access type ）ごとに関連付けられて構成されている。また、ユーザによる各操作命令ごとに、許可（Allowed ）と拒絶（Denied）とが定められている。

なお、図１、図２に示す例では、ＡＣＬ１２にはＲｅｑｕｉｒｅｍｅｎｔｓの項が入っているが、一般的なアクセス制御しかしないのであれば、ＡＣＬ１２はＲｅｑｕｉｒｅｍｅｎｔｓの項がないものであってよい。

【００２１】

このＡＣＬ１２は、ドキュメント１１を作成した作成者や、電子ファイル管理装置２の管理者（管理者権限を持つユーザ）が作成し、そのドキュメント１１に付与しておくこととする。装置本体２ａは、ドキュメント管理プログラム２１により、入力手段によるユーザからの各操作命令に対し、このＡＣＬ１２に基づいて、上述した各種の出力を行う。

【００２２】

次に、第１の実施形態にかかる電子ファイル管理装置２における電子ファイル格納時の動作について、図１（ａ）、図３、図４を参照して説明する。

【００２３】

ドキュメント管理プログラム２１がドキュメント１１とＡＣＬ１２とを受け取って保存する際、ドキュメント管理プログラム２１は受け取ったドキュメント１１とＡＣＬ１２をドキュメント保護プログラム２２に渡して保護ドキュメント１３を受け取る。

すなわち、ドキュメント保護プログラム２２は、受け取ったＡＣＬ１２に設定されているアクセス権限の制限と同一の制限がドキュメント１１にかけられるように、ドキュメント１１から保護ドキュメント１３を生成する。

【００２４】

このドキュメント保護プログラム２２による保護ドキュメント１３の生成（暗号化）とその復号化にかかるドキュメント保護・印刷システムの構成例を図３に示す。以下の説明では、この保護ドキュメント１３の活用（復号化）用途を、プリンタ３３により記録紙に印刷することであるとする。

【００２５】

この図３に示すドキュメント保護・印刷システムは、電子ファイル管理装置２、印刷用端末３１、プリンタ３３及びアクセスコントロールサーバ３２を有する。

電子ファイル管理装置２と印刷用端末３１は、表示装置（例えば、ＬＣＤ）、入力装置（例えば、キーボード）、外部記録装置（例えば、ＦＤＤ、ＨＤＤ）などを備えたコンピュータ端末を適用できる。なお、電子ファイル管理装置２にはドキュメント保護プログラム２２が、印刷用端末３１にはドキュメント印刷プログラム３１１がそれぞれ実装されている。

【００２６】

ドキュメント保護プログラム２２は、ドキュメントファイルに電子ファイル管理装置２の使用者（管理者）の入力操作に応じた印刷要件を設定するとともに、暗号化アルゴリズム（ＲＣ４、Ｔｒｉｐｌｅ　ＤＥＳ、ＩＤＥＡなど）を用いて

ドキュメントファイルを暗号化し、保護ドキュメントを生成する処理を行うプログラムである。

【００２７】

ドキュメント印刷プログラム３１１は、印刷用端末３１の使用者（ユーザ）の入力操作に応じ、保護ドキュメントを復号化するとともに設定されている印刷要件に応じた印刷処理をプリンタ３３に実行させる処理を行うプログラムである。

【００２８】

アクセスコントロールサーバ３２は、ユーザがドキュメントを印刷しようとする場合に、ドキュメント印刷プログラム３１１からの要求に応じてＡＣＬ１２を参照し、ドキュメントを印刷する権限があるか否か、印刷要件がどのように設定されているかを取得するサーバである。

アクセスコントロールサーバ３２には、ユーザ各人の認証用の情報（ユーザ名とパスワードとの組）が格納されたユーザデータベース３２１と、ユーザ各人ごとに設定された印刷要件を含むＡＣＬが登録されるＡＣＬデータベース３２２とが接続されている。

【００２９】

上述のシステムにおいて、ドキュメント１１とＡＣＬ１２とを取得したドキュメント保護プログラム２２は、上記の保護ドキュメント１３を生成するに当たって、ドキュメントファイルごとに固有のドキュメントＩＤ（Document ID）を生成し、復号に使用する暗号鍵（Key）とＡＣＬ１２とをこれに関連づけてアクセスコントロールサーバ３２へ送信し、登録する。

また、ドキュメント保護プログラム２２は、図４に示すように、暗号鍵を用いてドキュメント１１を暗号化し、その暗号化されたドキュメントファイル（暗号化ドキュメント）に対してドキュメントＩＤを付加して保護ドキュメント１３を生成する。

【００３０】

こうして保護ドキュメント１３が生成されると、ドキュメント管理プログラム２１は、受け取った保護ドキュメント１３をドキュメント１１及びＡＣＬ１２と共にドキュメント管理ＤＢ２３に格納する。こうして、電子ファイル管理装置２

は、ドキュメント１１と保護ドキュメント１３のペア（これをドキュメント・ペア（Ｄｏｃｕｍｅｎｔ　Ｐａｉｒ）と呼ぶ）にＡＣＬ１２を付与して（関連付けて）管理する。

【００３１】

次に、第１の実施形態にかかる電子ファイル管理装置２が、管理しているドキュメント・ペアに対してユーザからアクセス要求を受けた時の動作について、図１（ｂ）、図３を参照して説明する。

【００３２】

ドキュメント管理プログラム２１は、ユーザからドキュメント・ペアに対するアクセス要求を受けるとユーザの認証を行う。この認証では、ドキュメント管理プログラム２１は、ドキュメント・ペアに付与されているＡＣＬ１２を参照して、アクセスしてきたユーザに参照権限がある、すなわちｒｅａｄ権限があると判断すると、保護ドキュメント１３を返す。すなわち、装置本体２ａから上述のように表示手段などに出力する。

上記の認証で、アクセスしてきたユーザに参照権限がない、すなわちｒｅａｄ権限が認められていないとドキュメント管理プログラム２１が判断すると、表示手段にその旨を表示する。

【００３３】

この出力された保護ドキュメント１３の復号化について、上述した図３に示すドキュメント保護・印刷システムの例により説明する。

なお、図３の例では、ドキュメントファイルを印刷や参照しようとするユーザに対する上述の装置本体２ａからの出力として、管理者によりＦＤなどの情報記録媒体による受け渡しを行う場合と、通信網により印刷用端末３１へ送信する場合とを示している。

【００３４】

ユーザがドキュメントを印刷しようとする場合には、印刷用端末３１に保護ドキュメント１３を実装する。例えば、上述のように電子ファイル管理装置２から情報記録媒体に出力（記録）された保護ドキュメント１３を外部記録装置を用いて印刷用端末３１に読み取らせても良いし、印刷用端末３１が電子ファイル管理

装置２と通信可能である場合には、通信網を介して電子ファイル管理装置２から保護ドキュメント１３を印刷用端末３１に出力させるようにしてもよい。

【００３５】

ユーザが、印刷用端末３１の入力装置を介してドキュメント印刷プログラム３１１に対して印刷を指示すると、印刷を要求されたドキュメント印刷プログラム３１１は、ユーザを認証するために必要となるユーザ名とパスワードの入力をユーザに要求する。例えば、ドキュメント印刷プログラム３１１は、印刷用端末３１の表示装置にメッセージを表示するなどして、ユーザ名とパスワードの入力を要求する。

【００３６】

ドキュメント印刷プログラム３１１は、ユーザから入力されたユーザ名とパスワードとをアクセスコントロールサーバ３２へ送信して、ユーザ認証を要求する。

【００３７】

アクセスコントロールサーバ３２は、ドキュメント印刷プログラム３１１から受け渡されたユーザ名とパスワードとを用いてユーザ認証を行い、ユーザを特定する。

ユーザを特定すると、アクセスコントロールサーバ３２は、ＡＣＬデータベース３２２を参照し、ドキュメントファイルを印刷する権限がユーザにあるか否かや、ユーザがドキュメントファイルを印刷する際には、どのような印刷要件が設定されているかといった、アクセス権限の制限の情報を取得する。

ユーザにドキュメントファイル（保護ドキュメント１３）を印刷する権限がある場合、アクセスコントロールサーバ３２は、その旨を示す認証情報とともに、保護ドキュメント１３を復号化するための暗号鍵とユーザがドキュメントファイルを印刷する際の印刷要件とを印刷用端末３１を介してドキュメント印刷プログラム３１１に通知する。

【００３８】

アクセスコントロールサーバ３２から認証情報とともに、暗証鍵と印刷要件とを取得したドキュメント印刷プログラム３１１は、暗号鍵を用いて保護ドキュメ

ント１３を復号化してドキュメント１１に復元する。

そしてドキュメント印刷プログラム３１１は、印刷要件を満たすようにプリンタ３３に印刷処理を実行させる。例えば、ドキュメントファイルにＢＤＰが印刷要件として設定されている場合には、ドキュメントの内容とともに地紋を印刷する。

【００３９】

以上により、ドキュメントファイルを印刷する際に、管理者がユーザ各人に対して設定した印刷要件、すなわちＡＣＬ１２としてユーザ各人に対して設定したアクセス権限の制限を強制することが可能となる。

【００４０】

ここで、ドキュメント１１から保護ドキュメント１３を生成する際のドキュメント保護プログラム２２及びアクセスコントロールサーバ３２の動作、及び保護ドキュメント１３をドキュメント１１に復元して印刷する際のドキュメント印刷プログラム３１１及びアクセスコントロールサーバ３２の動作についてさらに詳しく説明する。

【００４１】

図４に、ドキュメント保護プログラム２２が保護ドキュメント１３を生成する際の動作を示す。ドキュメント保護プログラム２２は、電子ファイル管理装置２の入力装置における管理者の入力操作によってドキュメントファイルとＡＣＬ１２とを取得すると、ドキュメントファイルの暗号化・復号化するための暗号鍵を生成する。そして、ドキュメント保護プログラム２２は、生成した暗号鍵を用いてドキュメントファイルを暗号化して、暗号化ドキュメントを生成する。

【００４２】

さらにドキュメント保護プログラム２２は、ドキュメントファイルごとに固有のドキュメントＩＤを暗号化ドキュメントに添付して保護ドキュメント１３を生成する。

【００４３】

保護ドキュメント１３を生成した後、ドキュメント保護プログラム２２は電子ファイル管理装置２の通信機能を用いて、暗号鍵とＡＣＬ１２とドキュメントＩ

Ｄとをアクセスコントロールサーバ３２へ送信し、これらの登録をアクセスコントロールサーバ３２に要求する。

【００４４】

暗号鍵とＡＣＬ１２とドキュメントＩＤとをドキュメント保護プログラム２２から受け渡されたアクセスコントロールサーバ３２は、図５に示すように、これらを関連づけて一つのレコードとしてＡＣＬデータベース３２２に記録保持する。

【００４５】

なお、上記の例においてはドキュメントＩＤの生成や暗号鍵の生成をドキュメント保護プログラム２２が行う場合を示したが、これらの処理はアクセスコントロールサーバ３２や不図示のサーバなどで行っても良い。

また、電子ファイル管理装置２とアクセスコントロールサーバ３２との間が専用回線ではなくネットワーク網を介して接続されており、暗号鍵など送信する際に盗聴される懸念がある場合には、ＳＳＬ（Secure Socket Layer ）を用いて通信を行えばよい。

【００４６】

ドキュメント保護プログラム２２がアクセスコントロールサーバ３２と通信する際のプロトコルは、どのようなものを用いてもよい。例えば、分散オブジェクト環境を導入し、Ｊａｖａ（登録商標）　ＲＭＩ（Remote Method Invocation）やＳＯＡＰ（Simple Object Access Protocol ）をベースとして情報を送受信するようにしても良い。その場合、アクセスコントロールサーバ３２は、例えばregister(String docId,byte[] key,byte[] acl)のようなメソッドを実装するようにしてもよい。ＳＯＡＰであれば、ＨＴＴＰＳの上でＳＯＡＰプロトコルををやりとりし、ＲＭＩであればＳＳＬベースのSocketFactory を用いてＲＭＩを実行するようにすれば、ネットワーク上でのセキュリティを確保できる。

【００４７】

次に、ドキュメント印刷プログラム３１１が保護ドキュメント１３を印刷する際の動作について説明する。

図６に、保護ドキュメント１３を印刷する際のドキュメント印刷プログラム３

１１及びアクセスコントロールサーバ３２の動作の流れを示す。

ドキュメント印刷プログラム２１は、印刷用端末３１の入力装置におけるユーザの入力操作によって保護ドキュメント１３とユーザ名とパスワードとを取得すると、保護ドキュメント１３に添付されているドキュメントＩＤを取得する。

そして、ユーザ名とパスワードとドキュメントＩＤとアクセスタイプ（ユーザが要求する処理を示す情報。ここでは、保護ドキュメント１３を印刷しようとするので、"print" となる。）とをアクセスコントロールサーバ３２へ送信して、アクセス権限があるか否かのチェックを要求する。

【００４８】

アクセスコントロールサーバ３２は、ドキュメント印刷プログラム３１１からユーザ名とパスワードとドキュメントＩＤとアクセスタイプとを取得すると、ユーザデータベース３２１に登録されている情報を参照し、ユーザ認証を行う。

換言すると、アクセスコントロールサーバ３２は、ユーザデータベース３２１に登録されている情報を参照し、ドキュメント印刷プログラム３１１から取得した情報に含まれるユーザ名とパスワードとを組としたものが、ユーザデータベース３２１に組として登録されているか否かを判断する。

【００４９】

ユーザ認証に失敗した場合（換言すると、ドキュメント印刷プログラム３１１から受け渡された情報に含まれるユーザ名とパスワードとを組としたものがユーザデータベース３２１に登録されていない場合）、アクセスコントロールサーバ３２は、許可情報（ユーザが要求する処理を許可するか否かを示す情報）を「不許可」として印刷用端末３１へ送信し、ドキュメント印刷プログラム３１１へ受け渡す。なお、この場合は「エラー」とした許可情報をドキュメント印刷プログラム３１１へ受け渡すようにしてもよい。

【００５０】

一方、ユーザ認証に成功した場合、アクセスコントロールサーバ３２は、ＡＣＬデータベース３２２に格納されているレコードのうち、ドキュメント印刷プログラム３１１から取得した情報に含まれるドキュメントＩＤに関するレコードを読み出す。

【００５１】

アクセスコントロールサーバ３２は、読み出したレコードに含まれるＡＣＬ１２を取得し、ドキュメント印刷プログラム３１１から取得したユーザ名及びアクセスタイプに基づいて、ＡＣＬ１２から許可情報および印刷要件を取得する。

換言すると、アクセスコントロールサーバ３２は、ユーザ名とアクセスタイプとに基づいて、予めＡＣＬ１２に設定されている許可情報と印刷要件とを取得する。

【００５２】

ＡＣＬ１２から取得した許可情報が「許可」である場合、アクセスコントロールサーバ３２は、レコードに格納されている暗号鍵と印刷要件とを許可情報とともに印刷用端末３１へ送信してドキュメント印刷プログラム３１１に受け渡す。

一方、ＡＣＬ１２から取得した許可情報が「不許可」である場合、アクセスコントロールサーバ３２は、許可情報のみを印刷用端末３１へ送信してドキュメント印刷プログラムに受け渡す。

【００５３】

アクセスコントロールサーバ３２から許可情報を受け渡されたドキュメント印刷プログラム３１１は、取得した許可情報を参照し、「不許可」である場合には、印刷用端末３１の表示装置にメッセージを表示するなどして、要求された処理を実行できないことをユーザに通知する。

一方、取得した許可情報が「許可」である場合には、許可情報と共に受け渡された暗号鍵を用いて、保護ドキュメントのうちの暗号化ドキュメントの部分を復号化してドキュメントファイルに復元する。

【００５４】

また、ドキュメント印刷プログラム３１１は、許可情報と共に取得した印刷要件を満足するようにプリンタドライバを設定し（例えば、ＰＡＣが指定されていれば機密印刷モードに設定する）、プリンタ３３にドキュメントの印刷処理を実行させる。

なお、必要があれば、印刷用端末３１の表示装置にメッセージを表示するなどして、印刷パラメータの設定をユーザに要求するようにしてもよい。

【００５５】

アクセスコントロールサーバ３２から取得した印刷要件を満足する印刷をプリンタ３３では実行できない場合、換言すると、プリンタ３３がＡＣＬ１２に設定されていた印刷要件を満たす機能を備えていない場合には、その旨を示すメッセージを表示装置に表示させるなどしてユーザに通知し、印刷は行わずに処理を終了する。

【００５６】

以上の動作によって、ユーザごとに異なるアクセス権や印刷要件を設定することが可能となる。また、上記のように、サーバ側でドキュメントファイルに対するアクセス権限を判断するシステム構成においては、ＡＣＬデータベース３２２に登録されているＡＣＬ１２の内容を電子ファイル管理装置２やアクセスコントロールサーバ３２における入力操作によって変更できるようにてもよく、この場合には、保護ドキュメントを配布した後で印刷要件を変更したりすることが可能となる。

例えば、既に配布した保護ドキュメントに対するアクセス権限を新たなユーザに設定したり、特定のユーザに対して印刷要件を追加することなどが可能となる。

【００５７】

なお、本実施形態を用いる図３に示すドキュメント保護・印刷システムが上記のような手法でドキュメントファイルを保護していることを知っている者は、ドキュメント印刷プログラム３１１に成りすますプログラムをコンピュータ端末に実行させて暗号鍵を不正に入手し、保護ドキュメントを復号化することも可能ではある。この場合は、ＡＣＬ１２として設定されている印刷要件を強制されることなく、保護ドキュメントを印刷できてしまうこととなる。

【００５８】

このため、単に暗号鍵のみを用いてドキュメントファイルを暗号化するのではなく、ドキュメント保護プログラム２２の内部に埋め込まれた秘密鍵と暗号鍵とを合わせたもの（排他的論理和を取ったもの）でドキュメントファイルを暗号化することが好ましい。

この場合は、ドキュメント印刷プログラム３１１にも同一の秘密鍵を埋め込んでおくことで、管理者が設定した印刷要件を印刷時に強制するドキュメント印刷プログラム３１１のみが、保護ドキュメントを復号化して印刷することが可能となる。

【００５９】

また、図３を用いて上述したドキュメント保護・印刷システムにおいては、ドキュメント印刷プログラム３１１は、ドキュメントファイルの印刷に関する処理のみを行っているが、ドキュメント印刷プログラム３１１は、ドキュメントファイルの内容をユーザに提示したり、ドキュメントファイルを編集する機能を備えていても良い。例えば、Adobe Acrobat のplug-in としてこの機能を実現することが可能である。

【００６０】

なお、この第１の実施形態としての電子ファイル管理装置２では、上述した図２に示すＡＣＬ１２の例には記載していないが、ＡＣＬ１２のＡｃｃｅｓｓ　ｔｙｐｅとして例えばＧｅｔＯｒｉｇｉｎａｌ（オリジナル電子ファイルへのアクセス権限）を定義し、そのＧｅｔＯｒｉｇｉｎａｌのアクセス権限を認められているユーザがドキュメント・ペアにアクセスした場合には、ドキュメント管理プログラム２１は保護ドキュメント１３を返すのではなく、ドキュメント１１を返すようにしてもよい。

すなわち、電子ファイル管理装置２がＧｅｔＯｒｉｇｉｎａｌを定義されたＡＣＬ１２に基づいてユーザ認証を行い、アクセスしたユーザにＧｅｔＯｒｉｇｉｎａｌのアクセス権限が認められている場合にはドキュメント１１を装置本体２ａから上述のように出力するようにしてもよい。

【００６１】

また、ＡＣＬ１２にオリジナル電子ファイルであるドキュメント１１へのアクセス権限を定義しなくても、特別なユーザのみ（例えば保存したユーザのみ）がドキュメント１１へのアクセス権限を認められることとしてもよい。すなわち、ドキュメント管理プログラム２１が、予め設定された特別なユーザのみにドキュメント１１へのアクセス権限を認めることとしてもよい。

【００６２】

本実施形態によれば、ドキュメント管理プログラム２１により管理・格納されているドキュメントに対するアクセス制御（アクセス権限の制限）と、ユーザに渡された（電子ファイル管理装置２から出力された）ドキュメント（ポータブルドキュメント）へのアクセス制御とを統一することができる。

【００６３】

また、管理者はＡＣＬ１２としてアクセス権限の制限を設定し、ドキュメント１１とＡＣＬ１２とをドキュメント管理プログラム２１に渡すよう電子ファイル管理装置２を入力手段により操作するだけで、設定したアクセス権限に応じて保護ドキュメント１３をユーザに渡すよう電子ファイル管理装置に管理させることができる。

すなわち、管理者がＡＣＬ１２としてアクセス権限の制限を一度設定するだけで、電子ファイル管理装置２は、表示手段や外部記録装置などへの出力をそのアクセス権限の制限により管理することができる。

【００６４】

さらに、上述のようにオリジナル電子ファイルへのアクセス権限を定義することで、電子ファイル管理装置２は、上記したアクセス権限の制限による管理をドキュメント１１と保護ドキュメント１３とに対して行うことができる。すなわち、電子ファイル管理装置２は、ＡＣＬ１２として設定されたアクセス権限に応じてドキュメント１１又は／及び保護ドキュメント１３を出力するよう管理することができる。

【００６５】

なお、本実施形態は、入力されたデータがドキュメント１１だけからなるものであるのか、ドキュメント１１とＡＣＬ１２とからなるものであるのかをドキュメント管理プログラム２１で判定している。データがドキュメント１１だけからなる場合には、ドキュメント管理プログラム２１は、そのままドキュメント１１をドキュメント管理ＤＢ２３に登録する。このドキュメント１１に対する要求は、どのようなユーザであっても可能である。

【００６６】

次に、本発明の第２の実施形態としての電子ファイル管理装置５について、図７を参照して説明する。

この第２の実施形態は、ドキュメント管理プログラムが、第１の実施形態でドキュメント管理ＤＢ２３にドキュメント１１と保護ドキュメント１３（ドキュメント・ペア）をＡＣＬ１２に関連付けて格納していたのに替えて、保護ドキュメント１３を格納し、ドキュメント１１を破棄するものである。

すなわち、第１の実施形態のようにドキュメント１１を残しておくと、そのドキュメント１１にアクセス可能なユーザがプロテクトされていないドキュメント１１を流通させてしまう可能性がある。そのようなことが心配される環境では、この第２の実施形態とすることで保護ドキュメント１３を好適に管理することができる。なお、本実施形態においても、ＡＣＬの付加されていないドキュメント１１は、そのまま格納する。

【００６７】

この第２の実施形態の電子ファイル管理装置５における装置本体５ａは、物理的な構成は上述した第１の実施形態と同様であり、図７に示すように、ドキュメント管理プログラム５１と、ドキュメント保護プログラム２２と、ドキュメント管理ＤＢ２３と、をＨＤＤなどの記憶部（不図示）に備えてなる。

上述した第１の実施形態と同様のものについては同じ符号とし、説明を省略する。

また、ドキュメント保護プログラム２２がドキュメント１１から保護ドキュメント１３を生成する動作や、ユーザからのアクセスにより出力された保護ドキュメント１３を復号化してプリンタにより印刷する際のシステムや動作も、図３から図６を用いて上述したものと同様であってよい。

【００６８】

この第２の実施形態にかかる電子ファイル管理装置５における電子ファイル格納時の動作について、図７（ａ）を参照して説明する。

ドキュメント管理プログラム５１にドキュメント１１、またはドキュメント１１とＡＣＬ１２を渡し、ユーザが入力手段から格納するよう操作すると、ドキュメント管理プログラム５１は、受け取ったデータがドキュメント１１だけである

場合、そのままドキュメント管理ＤＢ２３に登録する。また、ドキュメント１１とＡＣＬ１２とを受け取った場合には、ドキュメント保護プログラム２２に渡して保護ドキュメント１３を受け取る。すなわち、上述のようにドキュメント保護プログラム２２に保護ドキュメント１３を生成させる。

生成された保護ドキュメント１３を受け取ると、ドキュメント管理プログラム５１は、受け取った保護ドキュメント１３をドキュメント管理ＤＢ２３に格納し、ドキュメント１１とＡＣＬ１２とは破棄する。

【００６９】

この第２の実施形態にかかる電子ファイル管理装置５が、管理しているドキュメントに対してユーザからアクセス要求を受けた時の動作について、図７（ｂ）を参照して説明する。

ドキュメント管理プログラム５１はドキュメントに対するアクセス要求を受けると、ドキュメント管理ＤＢ２３に格納している保護ドキュメント１３を返す。すなわち、装置本体５ａから上述のように表示手段などに出力する。

【００７０】

本実施形態では、ドキュメント１１は破棄され、保護ドキュメント１３はユーザによって読み出された後、ＡＣＬ１２に従ってアクセス制御されるため、ドキュメント管理プログラム５１でアクセス制御を行う必要はない。

しかし、保護ドキュメント１３を取得されると暗号を解読されて内容にアクセスされる可能性もあるため、その可能性を少しでも減らすために、上述した第１の実施形態と同様に、ドキュメント管理プログラム５１が保護ドキュメント１３をドキュメント管理ＤＢ２３に格納する際、保護ドキュメント１３にＡＣＬ１２を関連付けて格納（ＡＣＬ１２を付与して管理）し、そのＡＣＬ１２に基づいてアクセス制御を行うようにしてもよい。すなわち、上記したドキュメント１１を破棄する際に、ドキュメント管理プログラム５１はＡＣＬ１２を破棄せず、保護ドキュメント１３に関連付けてドキュメント管理ＤＢ２３に格納することとしてもよい。

このようにアクセス制御を行うことで、ドキュメント管理プログラム５１により管理・格納されているドキュメントに対するアクセス制御（アクセス権限の制

限）と、ユーザに渡された（装置本体５ａから出力された）ドキュメント（ポータブルドキュメント）へのアクセス制御とを統一することができる。

【００７１】

本実施形態によれば、暗号化されていないドキュメント１１を破棄することにより、管理しているドキュメントをより確実に保護することができる。

【００７２】

次に、本発明の第３の実施形態としての電子ファイル管理装置６について、図８を参照して説明する。

この第３の実施形態は、ドキュメント管理プログラムが、第１の実施形態でドキュメント保護プログラム２２に保護ドキュメント１３を生成させて、ドキュメント管理ＤＢ２３にドキュメント１１と保護ドキュメント１３（ドキュメント・ペア）をＡＣＬ１２に関連付けて格納していたのに替えて、ドキュメント１１をＡＣＬ１２に関連付けてそのまま格納し、ユーザからアクセス要求を受けた際にドキュメント保護プログラム２２に保護ドキュメント１３を生成させて上述のように出力するものである。

すなわち、第１の実施形態のような管理を行う場合、保護ドキュメント１３を保存しておく分だけディスク領域を多く必要とすることになる。そこで、この第３の実施形態は、ドキュメントへのアクセスがユーザから要求されたときに動的に保護ドキュメント１３を作成することで、余分なディスク領域を使用せずにすむ好適な管理を行うことができる。なお、本実施形態においてもドキュメント管理プログラム６１は、ＡＣＬが付加されていないドキュメント１１を受け取ると、このドキュメントをそのままドキュメント管理ＤＢ２３に登録する。

【００７３】

この第３の実施形態の電子ファイル管理装置６における装置本体６ａは、物理的な構成は上述した第１の実施形態と同様であり、図８に示すように、ドキュメント管理プログラム６１と、ドキュメント保護プログラム２２と、ドキュメント管理ＤＢ２３と、をＨＤＤなどの記憶部（不図示）に備えてなる。

上述した第１の実施形態と同様のものについては同じ符号とし、説明を省略する。

また、ドキュメント保護プログラム２２がドキュメント１１から保護ドキュメント１３を生成する動作や、ユーザからのアクセスにより出力された保護ドキュメント１３を復号化してプリンタにより印刷する際のシステムや動作も、図３から図６を用いて上述したものと同様であってよい。

【００７４】

この第３の実施形態にかかる電子ファイル管理装置６における電子ファイル格納時の動作について、図８（ａ）を参照して説明する。

ドキュメント管理プログラム６１にドキュメント１１とＡＣＬ１２を渡し、ユーザが入力手段から格納するよう操作すると、ドキュメント管理プログラム６１は、受け取ったドキュメント１１にＡＣＬ１２を付与してドキュメント管理ＤＢ２３に格納する。また、ドキュメント管理プログラム６１は、受け取ったデータがドキュメント１１だけであった場合には、このドキュメント１１をそのままドキュメント管理ＤＢ２３に登録する。

【００７５】

この第３の実施形態にかかる電子ファイル管理装置６が、管理しているドキュメントに対してユーザからアクセス要求を受けた時の動作について、図８（ｂ）を参照して説明する。

ドキュメント管理プログラム６１は、ドキュメントに対するアクセス要求を受けるとユーザ認証を行い、ドキュメント１１に付与されているＡＣＬ１２に基づいてそのユーザにアクセス権限があるかどうか確認する。そのユーザにアクセス権限がある場合、ドキュメント管理プログラム６１は、ドキュメント管理ＤＢ２３から指定されたドキュメント１１とＡＣＬ１２を取り出し、ドキュメント保護プログラム２２に渡して保護ドキュメント１３を上述のように生成させて受け取り、その生成された保護ドキュメント１３をドキュメント管理プログラム６１への呼び出し側へ返す。すなわち、装置本体６ａから上述のように表示手段などに出力する。

【００７６】

なお、この第３の実施形態においても、上述した第１の実施形態と同様に、ＡＣＬ１２のＡｃｃｅｓｓ　ｔｙｐｅとして例えばＧｅｔＯｒｉｇｉｎａｌ（オリ

ジナル電子ファイルへのアクセス権限）を定義し、装置本体６ａがユーザ認証を行うことで、ＧｅｔＯｒｉｇｉｎａｌのアクセス権限が認められているユーザに対して、保護ドキュメント１３ではなく、ドキュメント１１を返す（要求に応じて出力する）ようにしてもよい。

【００７７】

本実施形態によれば、ドキュメント管理プログラム６１により管理・格納されているドキュメントに対するアクセス制御（アクセス権限の制限）と、ユーザに渡された（装置本体６ａから出力された）ドキュメント（ポータブルドキュメント）へのアクセス制御とを統一することができる。

【００７８】

また、使用するディスク領域を保護ドキュメント１３の分だけ小さくすることができるため、ディスク容量が比較的小さい場合であっても好適な管理ができるようになる。

【００７９】

次に、本発明の第４の実施形態としての電子ファイル管理装置７について、図９を参照して説明する。

この第４の実施形態は、ドキュメント管理プログラムが、第１の実施形態でドキュメント保護プログラム２２に保護ドキュメント１３を生成させて、ドキュメント管理ＤＢ２３にドキュメント１１と保護ドキュメント１３（ドキュメント・ペア）をＡＣＬ１２に関連付けて格納していたのに替えて、予めドキュメント保護プログラム２２に保護ドキュメント１３を生成させて保存し、ドキュメント管理ＤＢ２３にドキュメント１１と保護ドキュメント１３（ドキュメント・ペア）をＡＣＬ１２に関連付けて格納するものである。

すなわち、電子ファイル管理装置７が内部でドキュメント保護プログラム２２を実行するのは、処理のパフォーマンス面から難しくなることも考えられる。そのような場合であっても、あらかじめドキュメント保護プログラム２２によってプロテクトした保護ドキュメント１３をドキュメント管理プログラム７１により保存することで、ドキュメント１１と保護ドキュメント１３を適切に管理することができるようにするものである。なお、本実施形態においてもドキュメント管

理プログラム６１は、ＡＣＬが付加されていないドキュメント１１を受け取ると、このドキュメントをそのままドキュメント管理ＤＢ２３に登録する。

【００８０】

この第４の実施形態の電子ファイル管理装置７における装置本体７ａは、物理的な構成は上述した第１の実施形態と同様であり、図９に示すように、ドキュメント管理プログラム７１と、ドキュメント保護プログラム２２と、ドキュメント管理ＤＢ２３と、をＨＤＤなどの記憶部（不図示）に備えてなる。

上述した第１の実施形態と同様のものについては同じ符号とし、説明を省略する。

また、ドキュメント保護プログラム２２がドキュメント１１から保護ドキュメント１３を生成する動作や、ユーザからのアクセスにより出力された保護ドキュメント１３を復号化してプリンタにより印刷する際のシステムや動作も、図３から図６を用いて上述したものと同様であってよい。

【００８１】

この第４の実施形態にかかる電子ファイル管理装置７における電子ファイル格納時の動作について、図９（ａ）を参照して説明する。

ユーザはまず、ドキュメント保護プログラム２２にドキュメント１１とＡＣＬ１２とを渡して保護ドキュメント１３を生成させる。

ドキュメント管理プログラム７１にドキュメント１１とＡＣＬ１２と生成された保護ドキュメント１３とを渡し、ユーザが入力手段から格納するよう操作すると、ドキュメント管理プログラム７１は、受け取ったドキュメント１１と保護ドキュメント１３（ドキュメント・ペア）をドキュメント管理ＤＢ２３に格納し、受け取ったＡＣＬ１２を付与して管理する。また、ドキュメント管理プログラム６１は、受け取ったデータがドキュメント１１だけであった場合には、このドキュメント１１をそのままドキュメント管理ＤＢ２３に登録する。

【００８２】

この第４の実施形態にかかる電子ファイル管理装置７が、管理しているドキュメントに対してユーザからアクセス要求を受けた時の動作について、図９（ｂ）を参照して説明する。

ドキュメント管理プログラム７１は、ドキュメント・ペアに対するアクセス要求を受けるとユーザ認証を行い、ドキュメント・ペアに付与されているＡＣＬ１２に基づいてアクセス権限があるかどうかを確認する。アクセス権限がある場合には、ドキュメント管理ＤＢ２３に格納している保護ドキュメント１３を返す。すなわち、装置本体７ａから上述のように表示手段などに出力する。

【００８３】

なお、この第４の実施形態においても、上述した第１の実施形態と同様に、ＡＣＬ１２のＡｃｃｅｓｓ　ｔｙｐｅとして例えばＧｅｔＯｒｉｇｉｎａｌ（オリジナル電子ファイルへのアクセス権限）を定義し、電子ファイル管理装置７がユーザ認証を行うことで、ＧｅｔＯｒｉｇｉｎａｌのアクセス権限が認められているユーザに対して、保護ドキュメント１３ではなく、ドキュメント１１を返す（要求に応じて出力する）ようにしてもよい。

【００８４】

また、この第４の実施形態では、ドキュメント保護プログラム２２は電子ファイル管理装置７に替えて、他の装置に実装されていてもよい。この場合、ドキュメント保護プログラム２２が実装された装置でドキュメント１１から保護ドキュメント１３を生成し、その生成を行った装置からネットワークや情報記録媒体などにより装置本体７ａにドキュメント１１と、保護ドキュメント１３と、ＡＣＬ１２とを渡すこととなる。

【００８５】

また、ドキュメント管理プログラム７１への保存の際にドキュメント１１と保護ドキュメント１３を両方渡すのではなく、保護ドキュメント１３のみを渡してドキュメント１１を破棄するようにしてもよい。この場合、ユーザからのアクセス要求を受けた際には、上述した第２の実施形態と同様の動作となる。

【００８６】

本実施形態によれば、ドキュメント管理プログラム７１により管理・格納されているドキュメントに対するアクセス制御（アクセス権限の制限）と、ユーザに渡された（装置本体７ａから出力された）ドキュメント（ポータブルドキュメント）へのアクセス制御とを統一することができる。

【００８７】

また、ドキュメント保護プログラム２２による保護ドキュメント１３の生成を、電子ファイル管理装置７における他の重い処理と同時にならないよう行うことができるため、電子ファイル管理装置７の処理能力が比較的低い場合であっても保護ドキュメント１３の生成などの処理を適切に行うことができる。

また、ドキュメント保護プログラム２２による保護ドキュメント１３の生成を他の装置で行うことにより、生成などの処理にかかる負担を効果的に分散させることができる。このことにより、電子ファイル管理装置７や上記他の装置の処理能力が比較的低い場合であっても、保護ドキュメント１３の生成などの処理を適切に行うことができる。

【００８８】

次に、上述した各実施形態で、印刷用端末３に接続されたプリンタ３３から機密印刷にて出力させる場合について説明する。

図１０に、上記各実施形態において適用されるプリンタが備えるセキュリティ機能の一部を示す。

【００８９】

まず、印刷要件としてＰＡＣが設定されている場合のドキュメント印刷プログラム３１の動作について説明する。ＰＡＣが設定されている場合のドキュメント印刷プログラム３１の動作を図１１に示す。

（１）ドキュメント印刷プログラム３１はＰＡＣが設定されているドキュメントファイルを印刷する際には、図１２に示すように、プリントダイアログを表示させた後に個人識別番号（Personal Identification Number：ＰＩＮ）を入力するダイアログを印刷用端末３の表示装置に表示させ、ユーザにＰＩＮの入力を要求する。

（２）印刷用端末３の入力装置を用いてユーザがＰＩＮを入力すると、ドキュメント印刷プログラム３１は、これをプリンタドライバ３３に設定し、印刷を指示する。

プリンタドライバ３３は、ドキュメントからPostscriptなどのＰＤＬ（Page Description Language）で記述された印刷データ（ＰＤＬデータ）を生成し、印

刷部数や出力トレイなどの印刷ジョブ情報を記述したＰＪＬ（Print Job Language）データをＰＤＬデータの先頭に付加する。プリンタドライバ３３はさらにＰＪＬデータの一部としてＰＩＮを付加し、そのＰＪＬデータ付きＰＤＬデータをプリンタ３３に送る。

プリンタ３３は、ＰＪＬデータ付きＰＤＬデータを受け取るとＰＪＬデータの内容を参照し、機密印刷用のＰＩＮが含まれている場合は印刷出力せずにプリンタ３内部の記憶装置（ＨＤＤなど）にＰＪＬデータ付きＰＤＬデータを保存する。ユーザがＰＩＮをプリンタ３３のオペレーションパネルを介して入力すると、プリンタ３３は入力されたＰＩＮをＰＪＬデータに含まれるＰＩＮと照合し、一致すればＰＪＬデータに含まれていた印刷ジョブ条件（部数、トレイなど）を適用しながらＰＤＬデータに従って印刷出力する。

（３）プリンタドライバ３３にＰＩＮが設定できない、すなわち、プリンタ３３が機密印刷をサポートしていない場合には、機密印刷をサポートしている別のプリンタを選択するようにユーザに通知し、ドキュメントを印刷せずに処理を終了する。

【００９０】

このようにすることで、印刷実行後、プリンタ３３のオペレーションパネルにおいて印刷実行前に入力したものと同一のＰＩＮが入力されるまでドキュメントのプリントアウトがプリンタ３３から出力されなくなる。このため、ドキュメントのプリントアウトがプリンタ３３に不用意に放置されることがなくなり、プリントアウトによるドキュメントの漏洩を防止することが可能となる。

さらに、ネットワーク上を流れるプリントデータを盗聴されないようにプリンタ３３とやりとりをＳＳＬで保護してもよい。

【００９１】

また、ドキュメント印刷プログラム３１をWindows（登録商標） Domainのユーザ管理と連動させて、ユーザに対してＰＩＮの入力を要求しないようにしてもよい。例えば、ＰＩＮをユーザに入力させるのではなく、Windows（登録商標） Domainから現在ログオン中のユーザＩＤを取得し、プリントデータとともにユーザＩＤをプリンタ３３へ送付するようにする。プリンタ３３は、オペレーションパ

ネルでユーザからのパスワード入力を受け、そのユーザＩＤとパスワードとでWindows（登録商標） Domainのユーザ認証機構を用いてユーザ認証を行い、成功すればプリントアウトするようにしても良い。Windows（登録商標） Domainに限定されず、予め導入されているユーザ管理と連動させることで、ユーザにとって面倒なＰＩＮ入力の手間を削減できる。

【００９２】

次に、印刷要件としてＥＢＣが設定されている場合のドキュメント印刷プログラム３１の動作について説明する。

（１）ドキュメント印刷プログラム２１は、ＥＢＣが設定されているドキュメントを印刷する際にドキュメントＩＤを示すバーコード画像データ（又は、二次元コード）のデータを生成する。

（２）ドキュメント印刷プログラム３１は、生成したバーコード画像データをスタンプ画像としてプリンタドライバ３３にセットし、プリンタ３３に印刷を指示する。

（３）プリンタドライバ３３にＥＢＣが設定できない、すなわち、プリンタ３がスタンプ機能をサポートしていない場合は、スタンプ機能をサポートしている他のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【００９３】

このようにすることで、ドキュメントのプリントアウトの各ページにはバーコードが印刷されるため、このバーコードを識別できる複写機、ファックス、スキャナのみがバーコードをデコードすることでドキュメントＩＤを取得し、そのドキュメントＩＤを基にアクセスコントロールプログラム３２が、ハードコピー、画像読み取り、ファックス送信などが許可されているか否かを判断することが可能となる。これにより、紙文書まで一貫したセキュリティ確保が可能となる。

【００９４】

次に、印刷要件としてＢＤＰが設定されている場合のドキュメント印刷プログラム３１の動作について説明する。

（１）ドキュメント印刷プログラム３１は、ＢＤＰが設定されているドキュメ

ントを印刷する際に、印刷を要求しているユーザ名と印刷日時とを文字列として取得する（例えば、Ichiro,2002/08/04 23:47:10）。

（２）ドキュメント印刷プログラム３１は、ドキュメントのプリントアウトを複写機で複写した際に、生成した文字列が浮き上がるように地紋画像を生成する。

（３）ドキュメント印刷プログラム３１は、生成した地紋画像をスタンプとしてプリンタドライバ３３にセットし、プリンタ３３にドキュメントの印刷を指示する。

（４）プリンタドライバ３３にＢＤＰが設定できない場合、すなわちプリンタ３３が地紋印刷をサポートしていない場合には、地紋印刷をサポートしている別のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【００９５】

このようにすることで、ドキュメントのプリントアウトの各ページには、印刷処理を実行したユーザ名と日時とが浮き出る地紋として印刷され、プリントアウトを複写機やスキャナ、ファックスで処理すると文字列が浮き出ることとなる。これ、ＥＢＣをサポートしていない複写機をしようする場合などに有効であり、ドキュメントのプリントアウトを複写することによる情報漏洩に対して抑止力を有する。

【００９６】

次に、印刷要件としてＳＬＳが設定されている場合のドキュメント印刷プログラム３１の動作について説明する。

（１）ドキュメント印刷プログラム３１は、ＳＬＳが設定されているドキュメントファイルを印刷する際に、予め用意された画像のうち、そのドキュメントの機密レベルに応じたもの（Top Secretならば「極秘」のマークなど）を選択する。

（２）選択した画像のデータを、スタンプとしてプリンタドライバ３３にセットし、プリンタ３３に印刷を指示する。

（３）プリンタドライバ３３にＳＬＳをセットできない場合、すなわち、プリンタ３３がＳＬＳをサポートしていない場合には、ラベルスタンプをサポートし

ている別のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【００９７】

このようにすることで、ドキュメントファイルのプリントアウトには、自動的に「極秘」や「マル秘」がスタンプとして印刷されるため、ドキュメントが機密文書であることが明らかとなる。すなわち、プリントアウトを所持する者に管理上の注意を喚起することができる。

【００９８】

上記の各例は、あくまでも印刷要件の一例であり、改ざん防止用の電子透かしを印刷するようにしたり、保護されているドキュメントは特殊な用紙に印刷する（印刷に使用する用紙トレイを特殊用紙のトレイに限定する）ようにしてもよい。

このように、プリンタ３３がサポートする様々なセキュリティ機能を利用してセキュリティポリシーを設定することによって、プリンタ３３のセキュリティ機能を無駄なく活用して、プリントアウトに至るまで一貫したセキュリティの確保が可能となる。これは上述した各実施形態のシステム構成においても同様である。

【００９９】

なお、上述した各実施形態は、本発明の好適な実施形態であり、本発明の主旨を逸脱しない範囲内において、種々変形して実施することが可能である。

例えば、上述した各実施形態で用いられる各種ドキュメント（電子ファイル）の内容は、文書に限定されず、例えば画像を含めた文書ファイルや画像ファイルなどであってもよい。

【０１００】

また、本発明に係る電子ファイル管理装置が入力手段と表示手段を備えることとしているが、装置本体が上述した動作をできればこの構成に限定されず、例えば、ネットワークを介して接続されたユーザ端末により装置本体がユーザからの入力を受けたり、ネットワークを介して接続された表示装置や外部記録装置に装置本体から出力したりしてもよい。

また、プリンタを装置本体や印刷用端末に接続して出力に用いる場合、ネットワークを介して接続されたものであっても、装置本体や印刷用端末と一体化されたものであってもよい。

【０１０１】

また、格納手段が複数ある場合、ＡＣＬ１２などが付与されていることを確認できるのであれば（例えば、上述のように関連付けて格納する、など）、ドキュメント・ペアのそれぞれやＡＣＬ１２を異なる格納部に格納してもよい。

【０１０２】

また、以上に、ドキュメント保護プログラムとしてユーザベース・アクセス制御モデルのものを利用した場合の実施形態について説明したが、アクセス権限を管理するための情報を設定して電子ファイルの管理を行うことができれば本発明はこのものに限定されない。例えば、ポリシーベース・アクセス制御モデルのドキュメント保護プログラムを利用した場合には、ＡＣＬではなくポリシーに従ってアクセスが制御されるだけで基本的には同じ仕組みとして本発明は同様に適用可能である。

【０１０３】

なお、上述した実施形態では、ドキュメント管理プログラム２１で入力したデータがドキュメント１１だけからなるのか、ドキュメント１１とＡＣＬ１２とからなるのかを判定し、ドキュメント１１だけであった場合には、このドキュメント１１をそのままドキュメント管理ＤＢ２３に格納している。しかしながら、ＡＣＬ１２が付加されているか否かに関わらず、すべてのドキュメントの保護ドキュメントを作成するものであってもよい。全てのドキュメントに対して保護ドキュメントを作成しておくことで、オリジナルドキュメントが作成者の許可なく変更される不具合を防止することができる。

【０１０４】

【発明の効果】

以上のように、本発明によれば、アクセス制限電子ファイルを、アクセス権限情報でアクセス権限を認められているユーザのみが復号可能であるように生成し、そのアクセス制限電子ファイルとオリジナル電子ファイルとを上記のアクセス

権限情報に基づいて管理することにより、アクセス権限情報でアクセス権限を認められていないユーザに対して、アクセス制限電子ファイルをたとえ入手したとしてもアクセスできないようにすることができると共に、そのアクセス権限の管理を、管理者（アクセス権限の設定者）がアクセス権限情報を作成するだけで自動的に行うことができる。

【図面の簡単な説明】

【図１】

本発明の第１の実施形態としての電子ファイル管理装置２におけるプログラムの構成の概要とその動作例を示すブロック図である。

【図２】

印刷要件を含んだＡＣＬの構造を例示する図である。

【図３】

保護ドキュメント１３を印刷に用いるための、保護ドキュメント１３の生成（暗号化）とその復号化にかかるシステムの構成例を示すブロック図である。

【図４】

ドキュメント保護プログラム２２が保護ドキュメント１３を生成する際の動作を示す図である。

【図５】

暗号鍵とＡＣＬ１２とドキュメントＩＤとを関連付けたレコードを例示する図である。

【図６】

保護ドキュメント１３を印刷する際のドキュメント印刷プログラム３１１及びアクセスコントロールサーバ３２の動作の流れを示す図である。

【図７】

本発明の第２の実施形態としての電子ファイル管理装置５におけるプログラムの構成の概要とその動作例を示すブロック図である。

【図８】

本発明の第３の実施形態としての電子ファイル管理装置６におけるプログラムの構成の概要とその動作例を示すブロック図である。

【図９】

本発明の第４の実施形態としての電子ファイル管理装置７におけるプログラムの構成の概要とその動作例を示すブロック図である。

【図１０】

プリンタが備えるセキュリティ機能の一例を示す図である。

【図１１】

ＰＡＣが設定されている場合のドキュメント印刷プログラム３１の動作例を示す図である。

【図１２】

ドキュメント印刷プログラム３１によりＰＡＣが設定されているドキュメントファイルを印刷する際の画面表示例を示す図である。

【符号の説明】

１１　ドキュメント（オリジナル電子ファイル）

１２　ＡＣＬ（アクセス権限情報）

１３　保護ドキュメント（アクセス制限電子ファイル）

２、５、６、７　電子ファイル管理装置

２ａ、５ａ、６ａ、７ａ　装置本体

２１、５１、６１、７１　ドキュメント管理プログラム（管理手段）

２２　ドキュメント保護プログラム（アクセス制限手段）

２３　ドキュメント管理ＤＢ（格納手段）

３１　印刷用端末

３１１　ドキュメント印刷プログラム

３２　アクセスコントロールサーバ

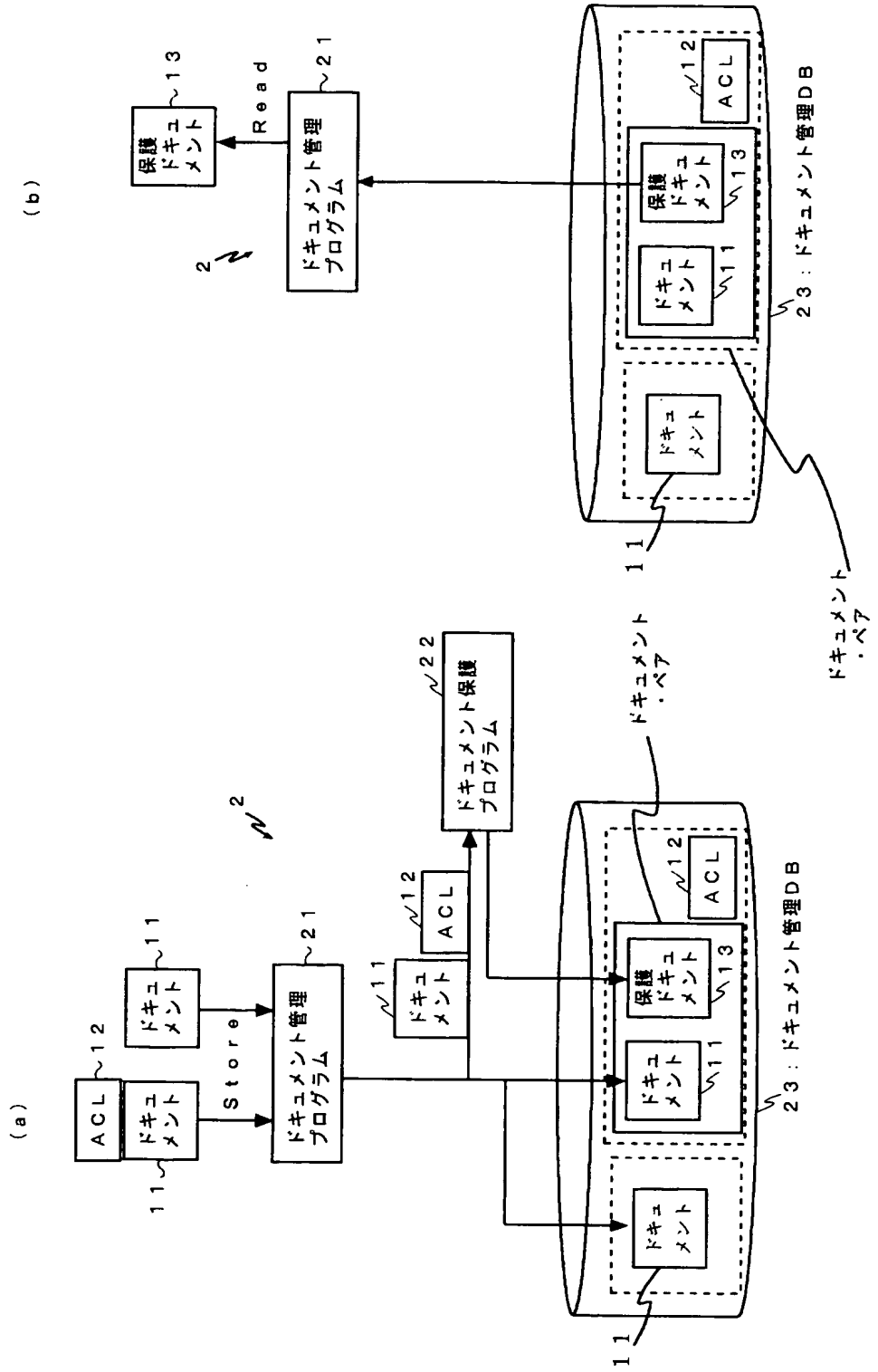
３２１　ユーザデータベース

３２２　ＡＣＬデータベース

３３　プリンタ

【書類名】　　図面

【図１】

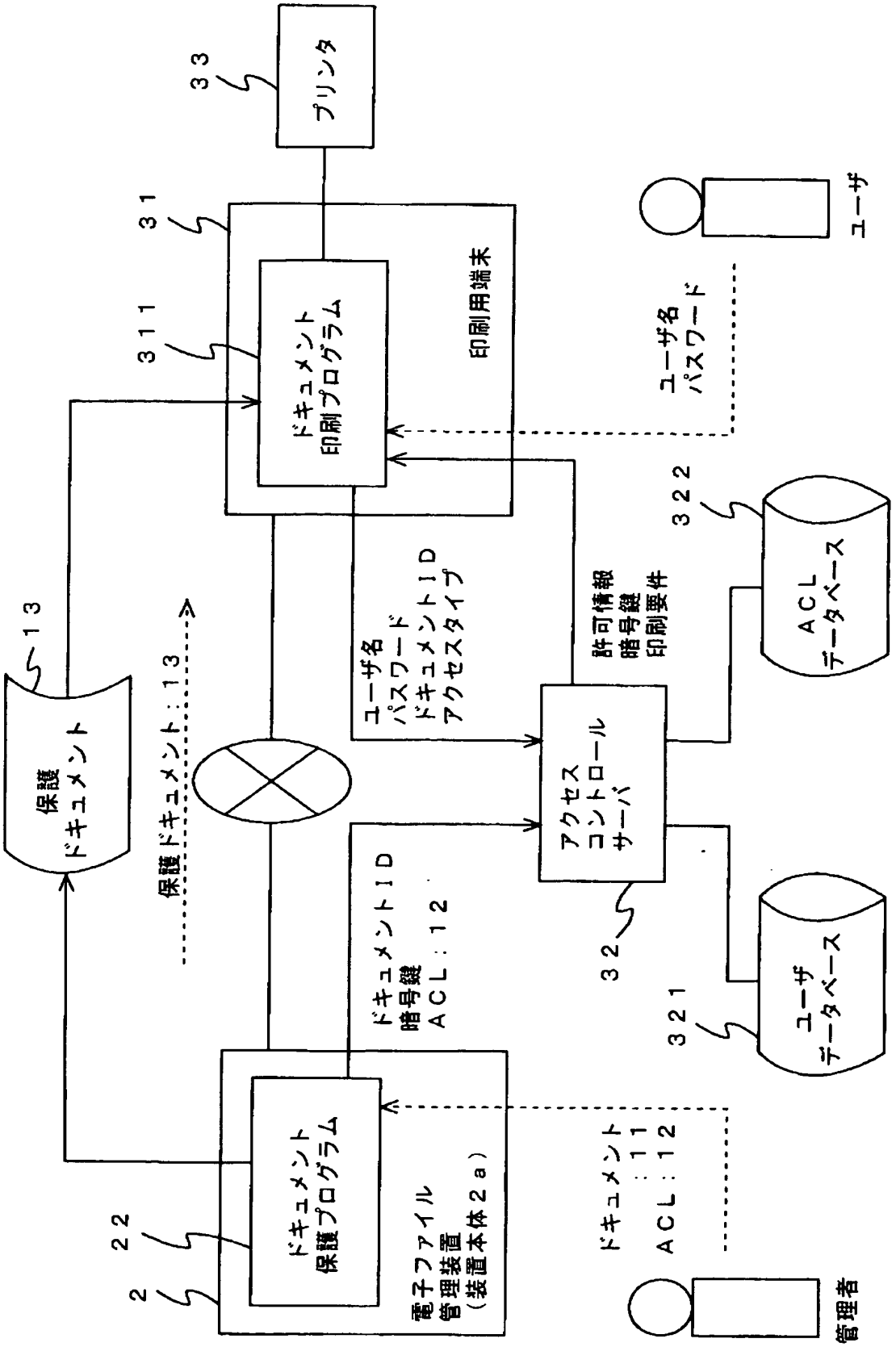

(a)
ACL
12
ドキュメント
11
Store
ドキュメント管理プログラム
21
2
ドキュメント保護プログラム
22
ドキュメント
11
ACL
12
ドキュメント・ペア
保護ドキュメント
13
23：ドキュメント管理DB
(b)
保護ドキュメント
13
Read
ドキュメント管理プログラム
21
2
ドキュメント・ペア

【図２】

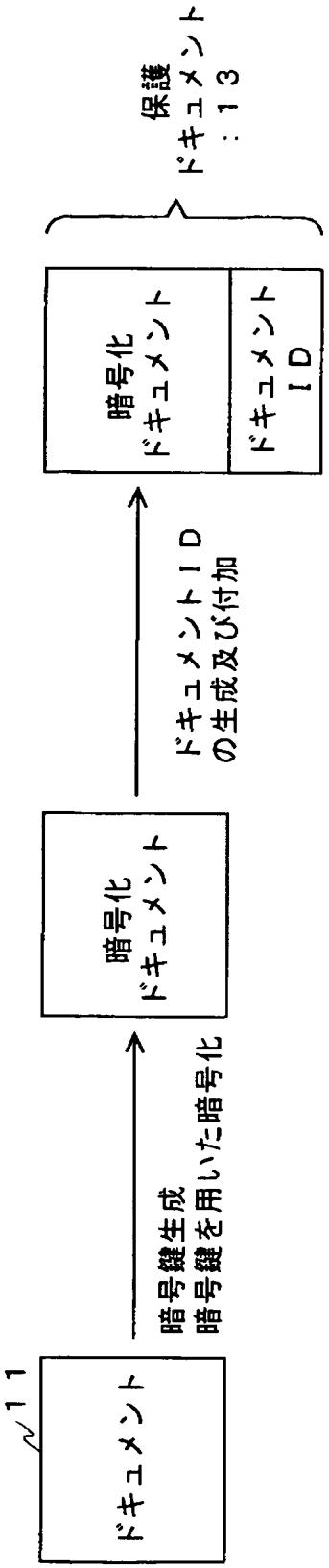
12

User name	Access type	Permission	Requirements
Ricoh	Read	Allowed	-
	Write	Denied	-
	Print	Allowed	PAC (Private Access)
			BDP (Background Dot Pattern)
			EBC (Embedding Barcode)
	Hardcopy	Allowed	RAD (Record Audit Data)
Taro	Read	Allowed	-
	Write	Denied	-
	Print	Denied	-
	Hardcopy	Denied	-

【図３】


プリンタ
33
31
311
ドキュメント
印刷プログラム
印刷用端末
ユーザ
ユーザ名
パスワード
322
ACL
データベース
許可情報
暗号鍵
印刷要件
ユーザ名
パスワード
ドキュメントID
アクセスタイプ
13
保護
ドキュメント
保護ドキュメント：13
アクセス
コントロール
サーバ
32
ドキュメントID
暗号鍵
ACL：12
321
ユーザ
データベース
22
2
ドキュメント
保護プログラム
電子ファイル
管理装置
（装置本体2a）
ドキュメント
：11
ACL：12
管理者

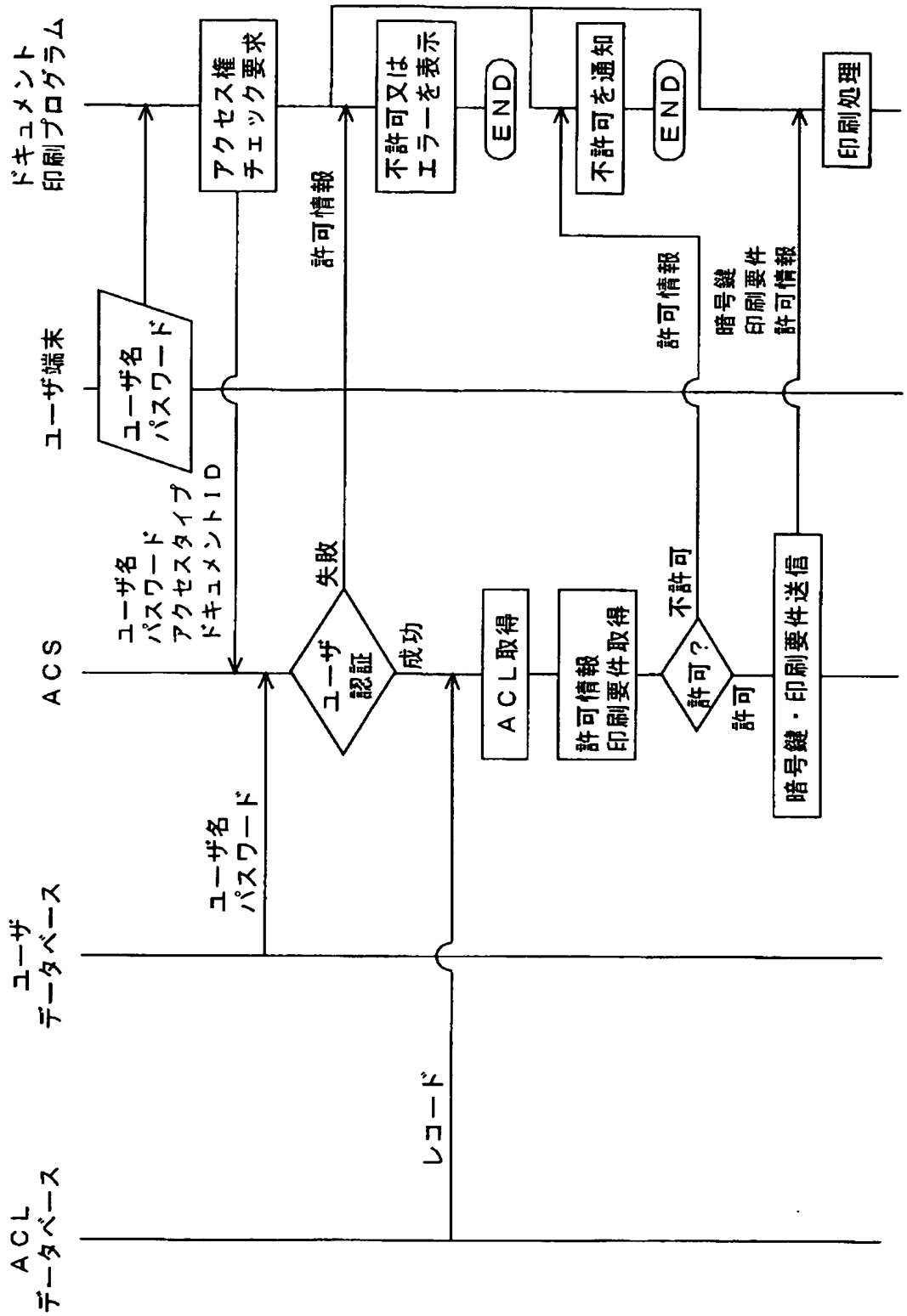
【図４】


保護
ドキュメント
：１３
暗号化
ドキュメント
ドキュメント
ＩＤ
ドキュメントＩＤ
の生成及び付加
暗号化
ドキュメント
暗号鍵生成
暗号鍵を用いた暗号化
１１
ドキュメント

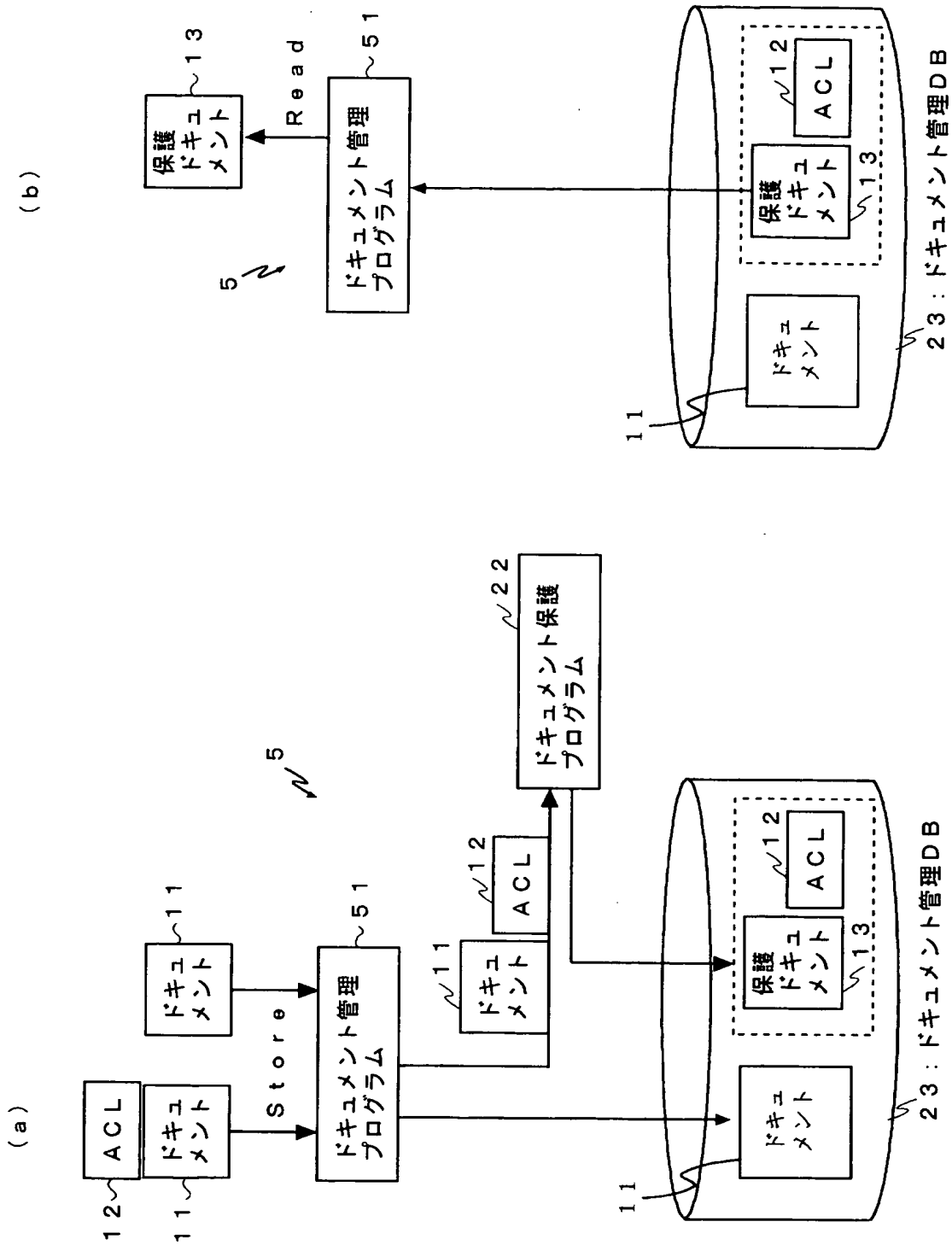
【図５】

Document ID	Key	ACL
133.139.234.23.22.125.98.192	89FECA8D2B	(binary data)
133.139.234.23.22.125.99.105	A73C44DA59	(binary data)

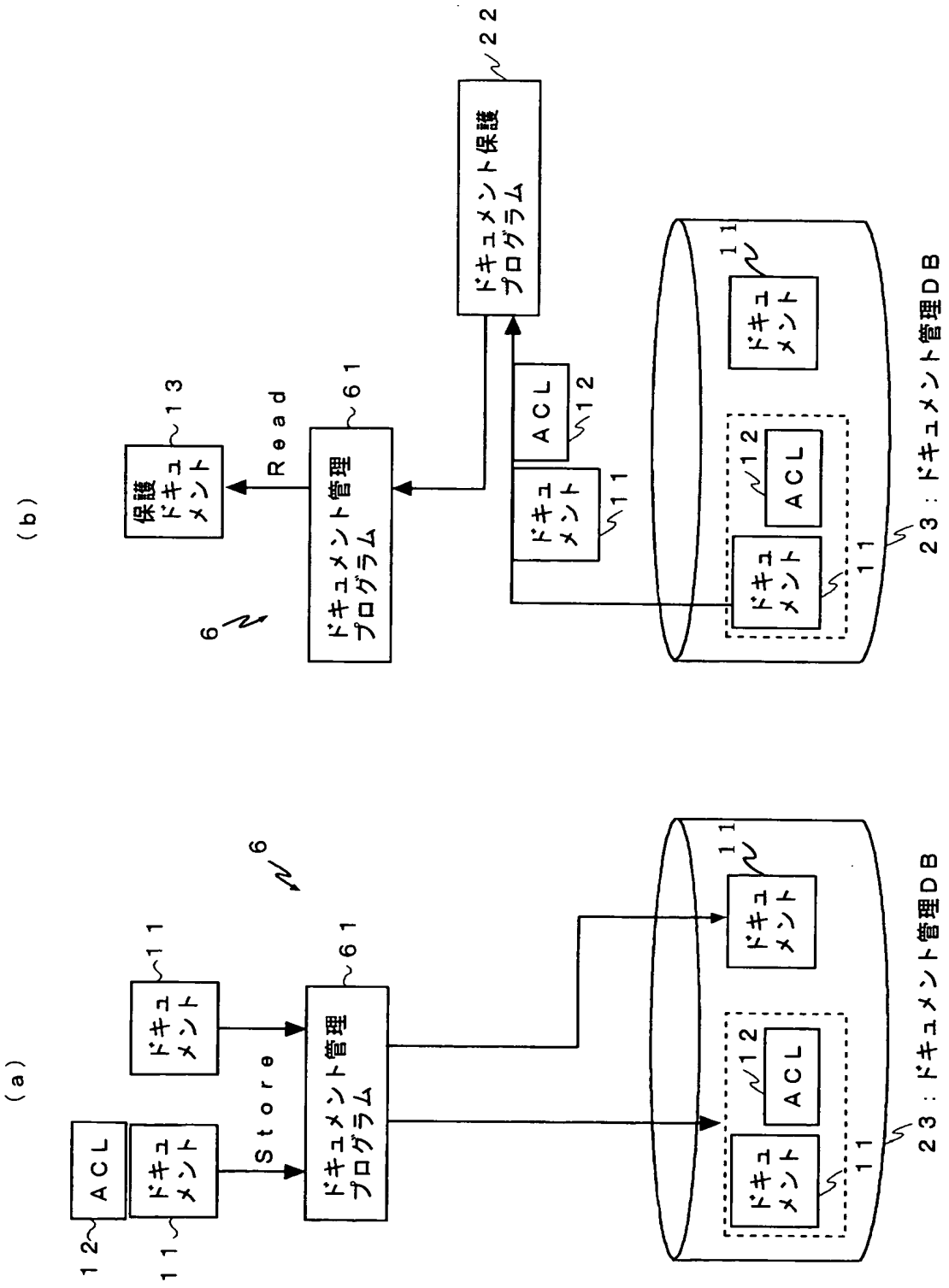
【図６】


ドキュメント
印刷プログラム
ユーザ端末
ＡＣＳ
ユーザ
データベース
ＡＣＬ
データベース
アクセス権
チェック要求
不許可又は
エラーを表示
ＥＮＤ
不許可を通知
ＥＮＤ
印刷処理
許可情報
ユーザ名
パスワード
ユーザ名
パスワード
アクセスタイプ
ドキュメントＩＤ
失敗
ユーザ
認証
成功
ＡＣＬ取得
許可情報
印刷要件取得
不許可
許可？
許可
暗号鍵・印刷要件送信
許可情報
暗号鍵
印刷要件
許可情報
ユーザ名
パスワード
レコード

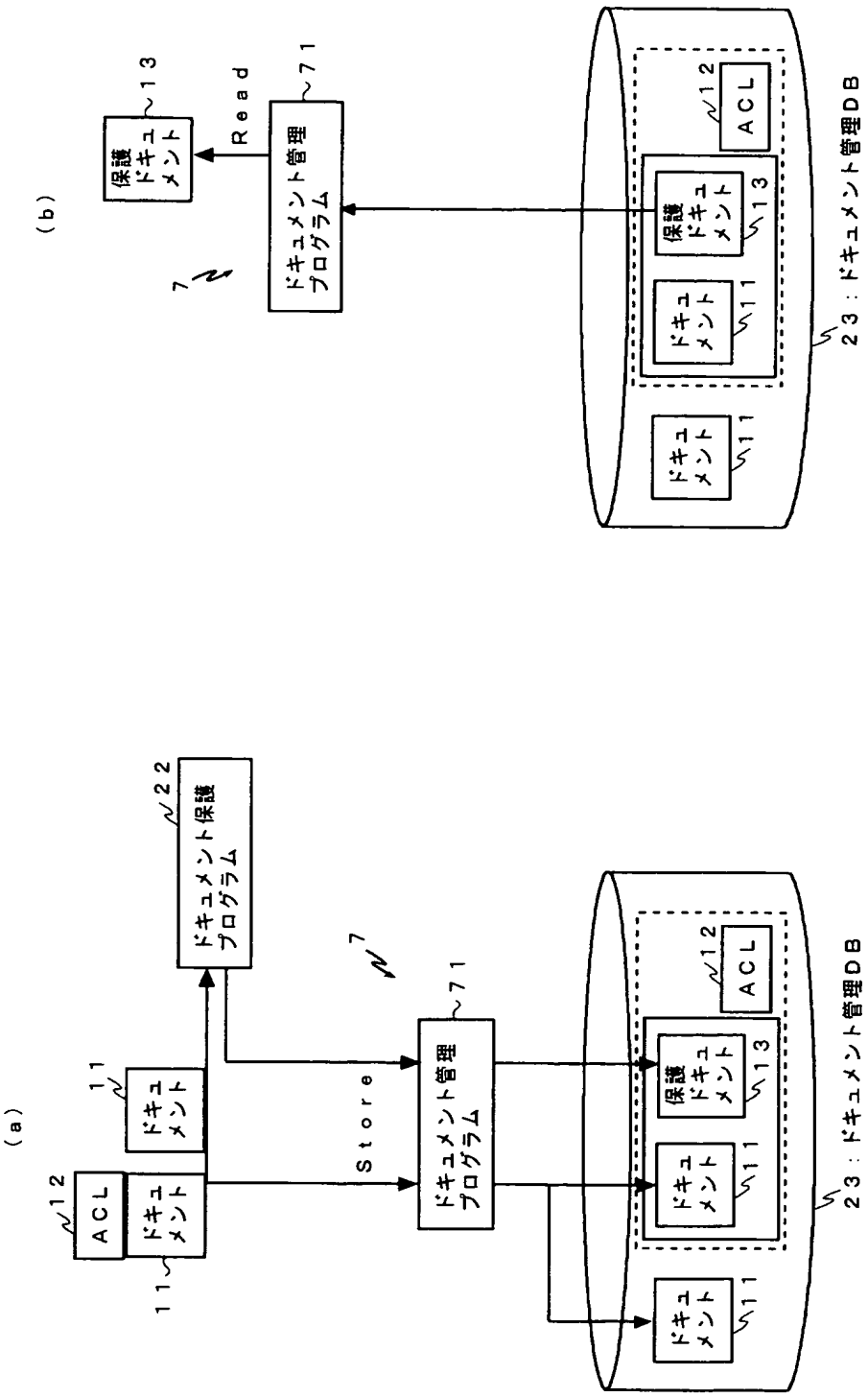
【図７】


(a)
ACL
ドキュメント
Store
ドキュメント管理プログラム
ドキュメント保護プログラム
保護ドキュメント
23：ドキュメント管理DB
(b)
Read
保護ドキュメント
ドキュメント管理プログラム
ドキュメント
ACL
11
12
13
22
51
5

【図８】


(a)
ACL
ドキュメント
12
11
Store
6
ドキュメント管理プログラム
61
ドキュメント
11
12
ACL
ドキュメント
11
23：ドキュメント管理DB
(b)
保護ドキュメント
13
Read
6
ドキュメント管理プログラム
61
ドキュメント保護プログラム
22
ACL
12
ドキュメント
11
ドキュメント
11
12
ACL
ドキュメント
11
23：ドキュメント管理DB

【図９】

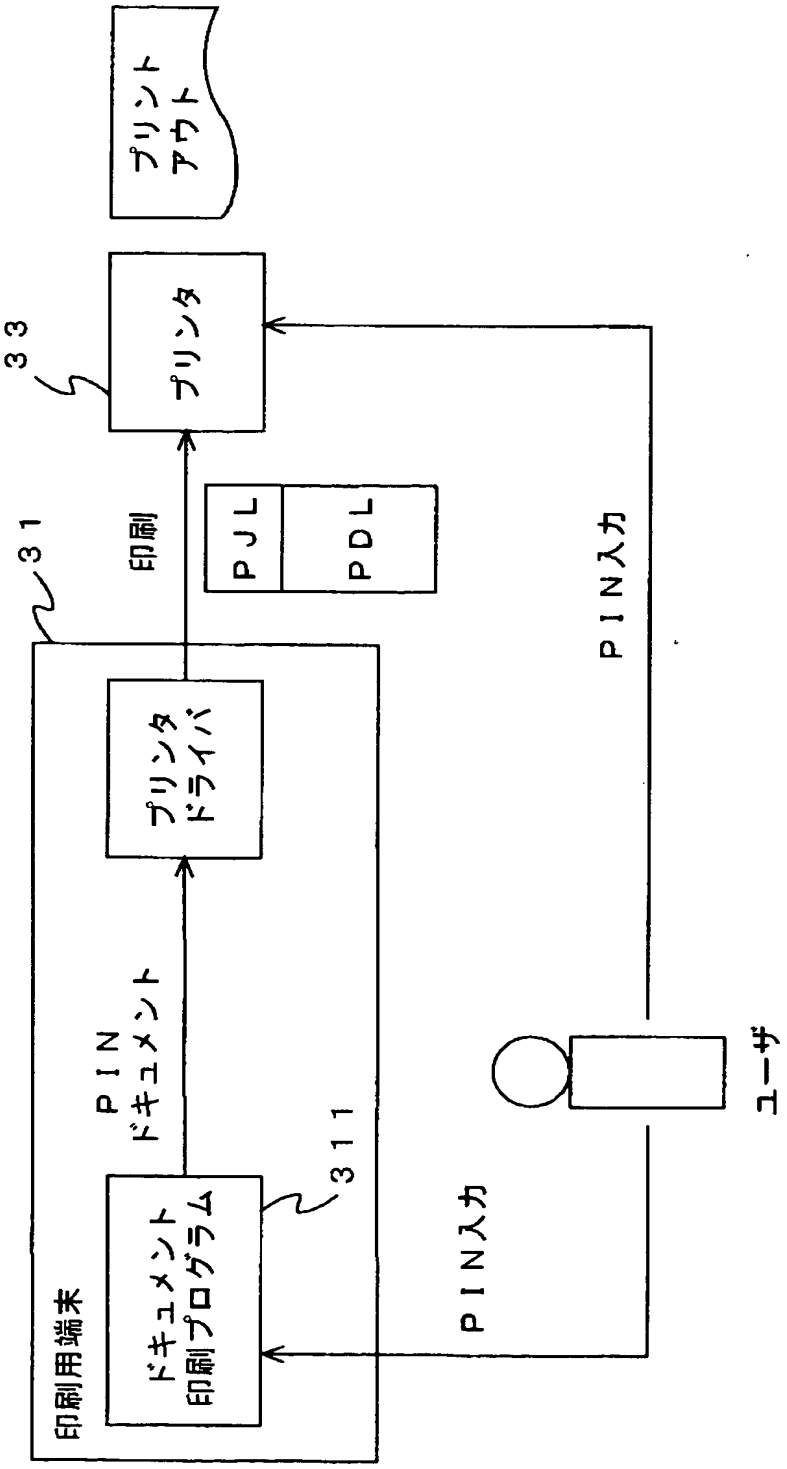

(b)
保護ドキュメント
13
Read
71
ドキュメント管理プログラム
7
12
ACL
保護ドキュメント
13
ドキュメント
11
ドキュメント
11
23：ドキュメント管理DB
(a)
ドキュメント保護プログラム
22
11
ドキュメント
12
ACL
ドキュメント
11
Store
7
71
ドキュメント管理プログラム
12
ACL
保護ドキュメント
13
ドキュメント
11
ドキュメント
11
23：ドキュメント管理DB

【図１０】

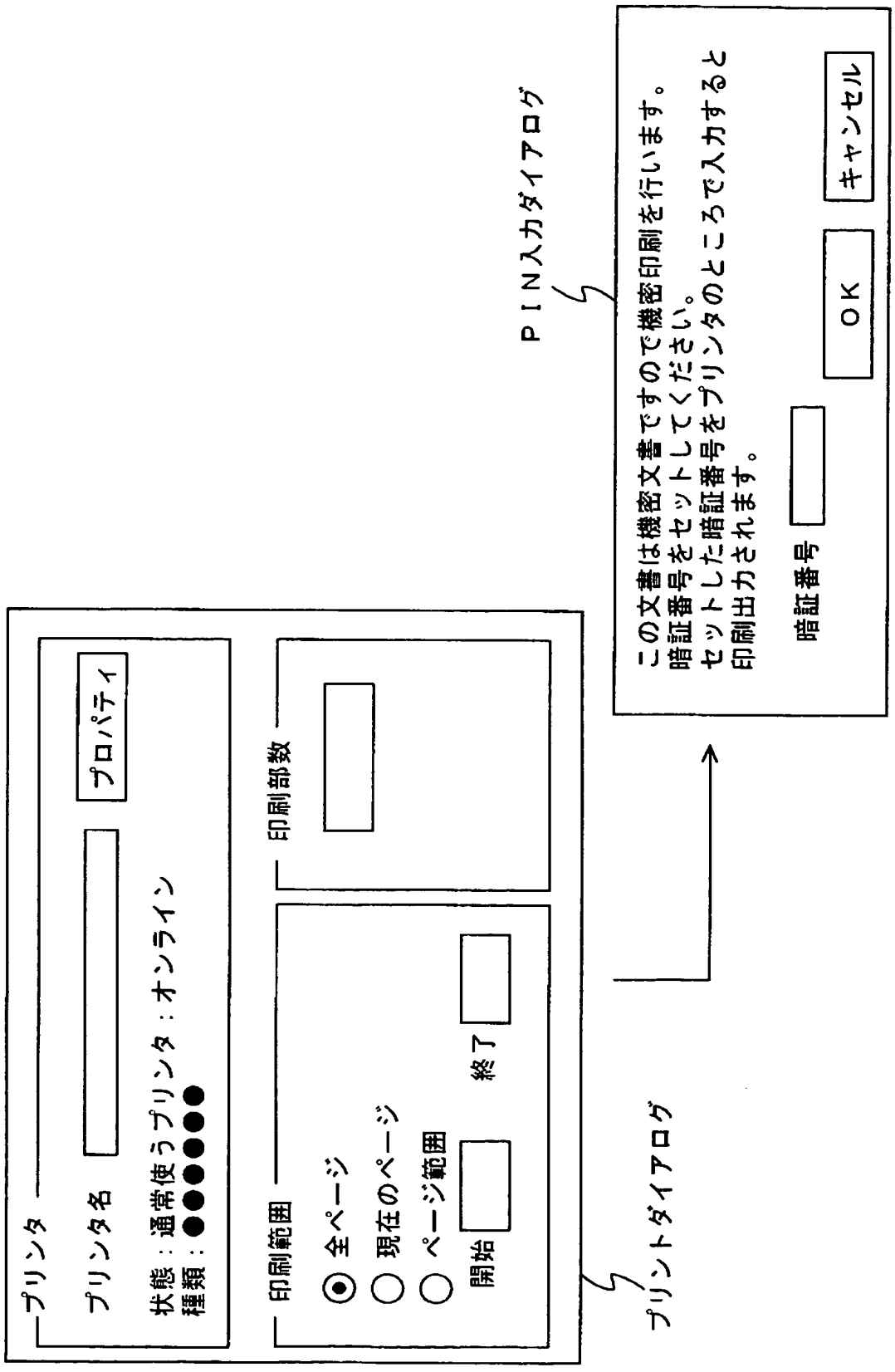
プリントセキュリティ機能

スタンプ機能	マル秘などのマークをスタンプやウォーターマークとしてページ内の任意の場所に重ねて印刷する機能。スタンプに使用することができるのは「秘」や「CONFIDENTIAL」などの文字列やビットマップ画像である。
地紋印刷機能	複写機で複写されると特定のイメージが浮き上がるようにコントロールした地紋画像を原稿に重ね合わせて印刷する機能。上記のスタンプ機能でスタンプとして指定する画像を地紋画像にすることで実現する手法が一般的である。
機密印刷機能	印刷を指示する際にプリンタドライバにＰＩＮ（Personal Identification Number）を指定すると、印刷した本人がプリンタのところへ行き、プリンタのオペレーションパネルでそのＰＩＮを入力しなければプリントアウトされない機能。

【図１１】


プリントアウト
33
プリンタ
印刷
PJL
PDL
31
PIN入力
プリンタドライバ
PIN
ドキュメント
311
ドキュメント印刷プログラム
印刷用端末
PIN入力
ユーザ

【図１２】


プリンタ
プリンタ名
プロパティ
状態：通常使うプリンタ：オンライン
種類：●●●●●●
印刷範囲
全ページ
現在のページ
ページ範囲
開始
終了
印刷部数
プリントダイアログ
PIN入力ダイアログ
この文書は機密文書ですので機密印刷を行います。
暗証番号をセットしてください。
セットした暗証番号をプリンタのところで入力すると
印刷出力されます。
暗証番号
OK
キャンセル

【書類名】　　要約書

【要約】

【課題】　オリジナルのドキュメントと、ユーザの権限に応じたアクセス制限を施した保護ドキュメントとをアクセス権限に応じて適切に管理することができるようにする。

【解決手段】　ドキュメント管理プログラム２１がドキュメント１１、またはドキュメント１１とＡＣＬ１２とを受け取って保存する際、ドキュメント管理プログラム２１は受け取ったドキュメント１１とＡＣＬ１２をドキュメント保護プログラム２２に渡し、プロテクトをかけられた保護ドキュメント１３を受け取る。ドキュメント管理プログラム２１は、ユーザからドキュメントに対するアクセス要求を受けると、ＡＣＬ１２に基づいてユーザの認証を行い、参照権限がある、すなわちｒｅａｄ権限があると判断すると、保護ドキュメント１３を返す。

【選択図】　　図１

特願２００２－２９９７２１

出　願　人　履　歴　情　報

識別番号　　［０００００６７４７］

１．変更年月日　　１９９０年　８月２４日
［変更理由］　　新規登録
住　所　　東京都大田区中馬込１丁目３番６号
氏　名　　株式会社リコー

２．変更年月日　　２００２年　５月１７日
［変更理由］　　住所変更
住　所　　東京都大田区中馬込１丁目３番６号
氏　名　　株式会社リコー